

PC/11304/50341

# Sertifikaat

REPUBLIEK VAN SUID AFRIKA

PATENT KANTOOR  
DEPARTEMENT VAN HANDEL  
EN NYWERHEID



# Certificate

REPUBLIC OF SOUTH AFRICA

PATENT OFFICE  
DEPARTMENT OF TRADE AND  
INDUSTRY

Hiermee word gesertifiseer dat  
This is to certify that

REC'D 11 JUN 2004

WIPO PCT

- 1) South African Patent Application No. **2003/2343** accompanied by a Provisional Specification was filed at the South African Patent Office on **26 March 2003** in the name of **Supersensor (Pty) Ltd** in respect of an invention entitled: "**Authentication of radio frequency transponders**".
- 2) The photocopy attached hereto is a true copy of the provisional specification and drawings filed with South African Patent Application No. **2003/2343**.

## PRIORITY DOCUMENT

SUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH RULE 17.1(a) OR (b)

Geteken te  
**PRETORIA**  
Signed at

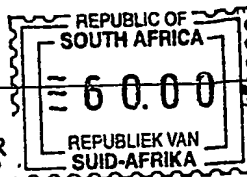
in die Republiek van Suid-Afrika, hierdie  
in the Republic of South Africa, this

6<sup>th</sup> dag van  
May 2004  
day of

  
.....  
Registrar of Patents

BEST AVAILABLE COPY

REPUBLIC OF SOUTH AFRICA				PATENTS ACT, 1978				
REGISTER OF PATENTS								
OFFICIAL APPLICATION NO.			LODGING DATE : PROVISIONAL			ACCEPTANCE DATE		
21	2003/2343		22	26 March 2003		43		
INTERNATIONAL CLASSIFICATION			LODGING DATE : COMPLETE			GRANTED DATE		
51			23					
FULL NAME(S) OF APPLICANT(S) / PATENTEE(S)								
71	SUPERSENSOR (PTY) LTD							
APPLICANTS SUBSTITUTED :						DATE REGISTERED		
71								
ASSIGNEE(S)						DATE REGISTERED		
71								
FULL NAME(S) OF INVENTOR(S)								
72	KRUGER, Johan							
	McMURRAY, John							
PRIORITY CLAIMED		COUNTRY		NUMBER		DATE		
N.B. Use international abbreviation for country. (See Schedule 4)		33		31		32		
TITLE OF INVENTION								
54	AUTHENTICATION OF RADIO FREQUENCY TRANSPONDERS							
ADDRESS OF APPLICANT(S) / PATENTEE(S)								
Unit 1, Block D, Gallagher Corner Richards Drive Midrand 1685 South Africa								
ADDRESS FOR SERVICE						REF		
74	D M Kisch Inc, 54 Wierda Road West, Wierda Valley, SANDTON						P26343ZA00	
PATENT OF ADDITION NO.				DATE OF ANY CHANGE				
61								
FRESH APPLICATION BASED ON				DATE OF ANY CHANGE				



Form P.1

REPUBLIC OF SOUTH AFRICA  
PATENTS ACT, 1978

APPLICATION FOR A PATENT AND ACKNOWLEDGEMENT OF RECEIPT  
(Section 30 (1) - Regulation 22)  
The grant of a patent is hereby requested by the undermentioned applicant  
on the basis of the present application filed in duplicate.

PBHR  
229

## OFFICIAL APPLICATION NO

21 01 4003/2343

## DMK REFERENCE

P26343ZA00

## FULL NAME(S) OF APPLICANT(S)

71

SUPERSENSOR (PTY) LTD

## ADDRESS(ES) OF APPLICANT(S)

Unit 1, Block D, Gallagher Corner  
Richards Drive  
Midrand  
1685  
South Africa

## TITLE OF INVENTION

54

AUTHENTICATION OF RADIO FREQUENCY TRANSPONDERS

THE APPLICANT CLAIMS PRIORITY AS SET OUT ON THE ACCOMPANING FORM P2  
The earliest priority claimed is

THIS APPLICATION IS FOR A PATENT OF  
ADDITION TO PATENT APPLICATION NO.

21 01

THIS APPLICATION IS FRESH APPLICATION IN TERMS  
OF SECTION 37 AND BASED ON APPLICATION NO.

21 01

## THIS APPLICATION IS ACCOMPANIED BY :

- |   |     |  |
|---|-----|--|
| X | 1a  | A single copy of a provisional specification of 10 pages.                |
|   | 1b  | Two copies of a complete specification of pages.                         |
|   | 2a  | Informal drawings of sheets.   |
| X | 2b  | Formal drawings of 3 sheets.   |
|   | 3   | Publication particulars and abstract (form P8 in duplicate).             |
|   | 4   | A copy of figure of the drawings for the abstract.                       |
|   | 5   | Assignment of invention (from the inventors) or other evidence of title. |
|   | 6   | Certified priority document(s).  |
|   | 7   | Translation of priority document(s).                                     |
|   | 8   | Assignment of priority rights.   |
|   | 9   | A copy of form P2 and a specification of S.A. Patent Application.        |
|   | 10  | A declaration and power of attorney on form P3.                          |
|   | 11  | Request for ante-dating on form P4.                                      |
|   | 12  | Request for classification on form P9.                                   |
|   | 13a | Request for delay of acceptance on form P4.                              |
|   | 13b |  |

21 01

DATED

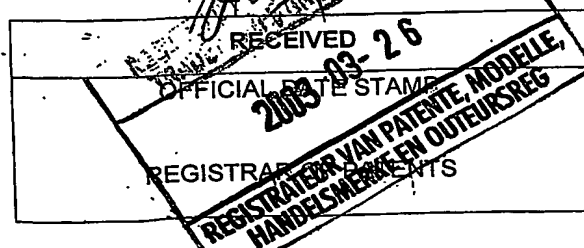
26 March 2003

## ADDRESS FOR SERVICE

74

D M Kisch Inc  
Inanda Greens Business Park  
54 Wierda Road West  
Wierda Valley  
SANDTON

Patent Attorney for Applicant(s)



The duplicate will be returned to the applicant's address for service as

## REPUBLIC OF SOUTH AFRICA

## PATENTS ACT, 1978

PROVISIONAL SPECIFICATION  
( Section 30 (1) - Regulation 27 )

OFFICIAL APPLICATION NO.		LODGING DATE		DMK REFERENCE
21	2003/2343	22	26 March 2003	P26343ZA00

FULL NAME(S) OF APPLICANT(S)	
71	SUPERSENSOR (PTY) LTD

FULL NAME(S) OF INVENTOR(S)	
72	KRUGER, Johan McMURRAY, John

TITLE OF INVENTION	
54	AUTHENTICATION OF RADIO FREQUENCY TRANSPONDERS

## **INTRODUCTION AND BACKGROUND**

THIS invention relates to electronic identification systems and more particularly to such systems including radio frequency (RF) transponders and associated readers, interrogators and verifiers therefor.

5

A system of the aforementioned kind is typically used to mark and identify products or goods, and would further include a plurality of encoder units for writing data into respective memory arrangements of the transponders. In use, a transponder is attached to a product item and the data written into the transponder may relate to the kind of product, the date of manufacture and/or any other data relating to the product. Normally the data is written into the memory arrangement at the source of the product, but in some applications additional data may be written into the memory arrangement at various points along a distribution chain. Of course the data written into the memory arrangement can at any stage be read with a verifier, interrogator or reader.

5

In some applications, security arrangements are required which would prevent unauthorized parties from attaching non-genuine transponders (purporting to store data encoded by an authorised encoder) to grey or infringing goods, thereby facilitating passing the grey goods off as genuine goods.

20

## **OBJECT OF THE INVENTION**

Accordingly, it is an object of the present invention to provide a system and

method with which the applicant believes transponders originating from an authorized source could be distinguished from non-genuine transponders.

### **SUMMARY OF THE INVENTION**

- 5 According to the invention there is provided an electronic identification system comprising:
- a plurality of transponders;
  - at least one transponder encoder for writing respective first watermark data into a memory arrangement of each transponder;
  - 10 - at least one verifier for interrogating a selected transponder and to read data stored in the transponder;
  - said first watermark being derived from an algorithm and input data;
  - the verifier comprising computing means configured to retrieve the algorithm and the input data and to compute second watermark data for
  - 15 comparison with the first watermark data.

The algorithm may be an encryption algorithm and the input data may comprise at least one of a constant and a variable.

- 20 The system may further comprise at least one conventional reader for reading the data transmitted, but which does not comprise the computing means configured as aforesaid.

Hence, the at least one verifier is used for verification of the authenticity of a transponder and the at least one conventional reader merely for reading data transmitted by the transponder when interrogated.

- 5 The data transmitted by the transponder may comprise the first watermark data and identification code data associated with the transponder.

The at least one verifier may utilize said identification code data to retrieve the algorithm and the input data from memory means of the verifier.

10

At least part of the input data may alternatively or in addition be derived from sensor means response to a parameter of the response signal or a communications channel with the transponder.

15

According to another aspect of the invention there is provided a method of authenticating a transponder of an electronic identification system, the method comprising the steps of:

20

- writing into a memory arrangement of the transponder first watermark data derived from an algorithm and input data for the algorithm;
- interrogating the transponder by causing the transponder to transmit to a verifier a response signal comprising data stored in the memory arrangement of the transponder;
- utilizing at the verifier the transmitted data to retrieve the algorithm and

the input data;

- utilizing the retrieved algorithm and input data to compute second watermark data; and
- comparing the first watermark data and the second watermark data to give an indication of the authenticity of the transponder.

5

The first watermark data may be generated by an encoder and may then be written into the memory arrangement of the transponder.

10

The encoder may be connectable to a central station for downloading into a memory arrangement of the encoder a set of algorithms comprising said algorithm.

5

The central station and/or encoder may further be configured to write the set of algorithms and input data for the set of algorithms into a memory arrangement of the verifier. Said algorithm and said input data for said algorithm may be stored in the verifier in relation to identification code data of the transponder.

20

The input data may be arbitrarily selected data and may be changed by the encoder from time to time.

The data transmitted to the verifier in the response signal may comprise said



identification code data of the transponder. The identification code data may be utilized by the verifier to retrieve said algorithm and said input data.

The input data for said algorithm may further comprise data derived by the verifier from a parameter of said response signal or a communications channel with the transponder.

In some forms of the method the step of comparing the first watermark data and the second watermark data may be performed on the verifier. In these cases, the first watermark data is transmitted by the transponder to the verifier.

In other forms of the method the step of comparing the first watermark data and the second watermark data may be performed on the transponder. In these cases, the second watermark data would be computed on the verifier and then transmitted to the transponder where the comparison is performed. The transponder may then provide the indication of the authenticity of the transponder.

## **BRIEF DESCRIPTION OF THE ACCOMPANYING DIAGRAMS**

The invention will now further be described, by way of example only, with reference to the accompanying diagrams wherein

figure 1 is a block diagram of an electronic identification system according

to the invention;

figure 2 is a more detailed block diagram of an encoder, a transponder and a verifier of the system; and

figure 3 is a diagram illustrating different aspects of the method according to the invention.

### **DESCRIPTION OF PREFERRED EMBODIMENTS OF THE INVENTION**

In figure 1 there is shown a block diagram of an electronic radio frequency identification (RFID) system according to the invention designated 10.

The system comprises a brand owner central computer system (BOCS) 12 of a brand owner of articles to be tagged and/or marked with transponders 14.1, 14.2, 14.3, to 14.n of the system. The system further comprises a plurality of encoder devices 16.1. to 16.n which are proprietary to and controlled by the brand owner. The system still further comprises a plurality of conventional readers or interrogators 18 for reading the transponders in well-known manner. The reader is caused to broadcast an RF interrogation signal 20 towards a transponder population 14. The transponders are energized in well-known manner by the signal and each causes a response signal comprising respective identification code data stored in a memory arrangement of the transponder to be transmitted to the reader. The reader receives the response signal, extracts the data and identify and/or count the transponder utilizing said data.

The system further comprises a plurality of verifiers 22 which are proprietary to and/or controlled by the aforementioned brand owner.

5 In the system according to the invention, first watermark data is in addition to the aforementioned ID data electronically written to and stored in the memory arrangement of the transponder. The first watermark data is so written into the transponder by an encoder 16.1 as will hereinafter be described with reference to figure 2.

10 The first watermark is derived from an algorithm and input data for the algorithm. A set of algorithms and associated input data is written by BOCS 12 into a memory arrangement 24 of the encoder 16. The encoder computes the first watermark data by selecting one algorithm of said set of algorithms and associated input data. Data relating to the selected algorithm and input data are also written into a memory arrangement 26 of verifier 22. The first watermark data is downloaded into and stored in a memory arrangement 28 of the transponder as shown at 30 in figure 2.

20 To verify the authenticity of the transponder 14.1, the verifier 22 is used as hereinafter described. Normal and conventional reading of the ID code data of the transponder is performed with conventional reader 18 shown in figure 1. The verifier 22 is caused to transmit an interrogation signal 32 to the transponder. The transponder derives power from this signal and transmits a

response signal 34 carrying or embodying the ID code data. The controller 36 of the verifier utilizes the ID code data to retrieve from memory arrangement 26 the algorithm and input data associated with transponder 14.1. The computing means of the verifier then utilizes the retrieved algorithm and associated input data to compute second watermark data. The verifier thereupon transmits at 38 the computed second watermark data to the transponder 14.1.

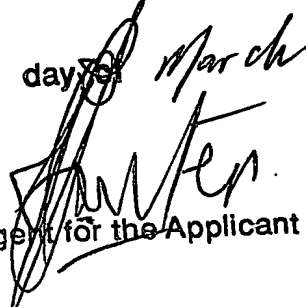
The controller 40 of the transponder 14.1 is configured to compare the stored first watermark data and the received second watermark data. If the compared data correspond, the transponder 14.1 provides a first indication to the verifier 22 at 40 and if the data do not correspond, a second indication is provided.

In other forms of the method, the transponder 14.1 is caused to transmit with the response signal 34, the first watermark data to the verifier 22. The comparison between the first watermark data and the second watermark data computed by the verifier is then performed by computing means 36 on the verifier 22. The verifier would then also generate one of the aforementioned first and second indications, depending on an outcome of the comparison.

The aforementioned input data for the algorithm may comprise at least one of a constant and a variable. The constant may be an arbitrarily selected number and need not have any direct relation with the ID code data. The set of

algorithms, constants and variables may all be downloaded into the encoder and the verifier as hereinbefore described. This is illustrated by the lines designated a in figure 3. In other forms of the method, the variable may be a parameter of a signal 32, 34 or a communications channel between the transponder 14.1 and the verifier 22 and may in effect be carried by the transponder to be available to both the encoder and the verifier. This aspect is illustrated by the lines designated b in figure 3. In still further forms, at least part of the input data for the algorithm may be transferred from the central computer or encoder to the verifier and that data may be retrieved by the verifier, before computing the second watermark data.

It will be appreciated that there are many variations in detail on the system, the encoder, verifier, transponder and method according to the invention without departing from the scope and spirit of this disclosure.

Dated this 26 day of March 2003  
  
Patent Attorney / Agent for the Applicant

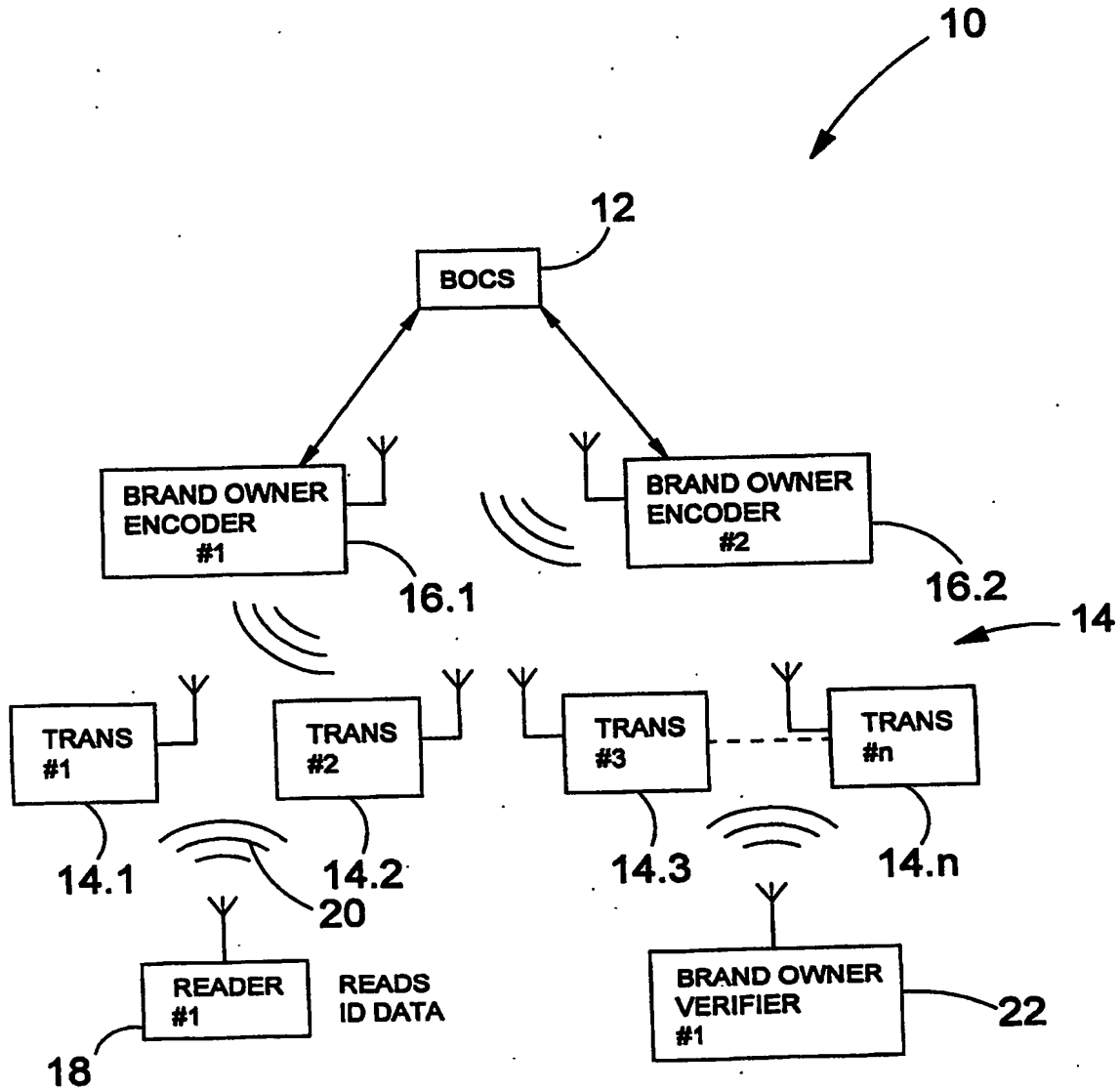
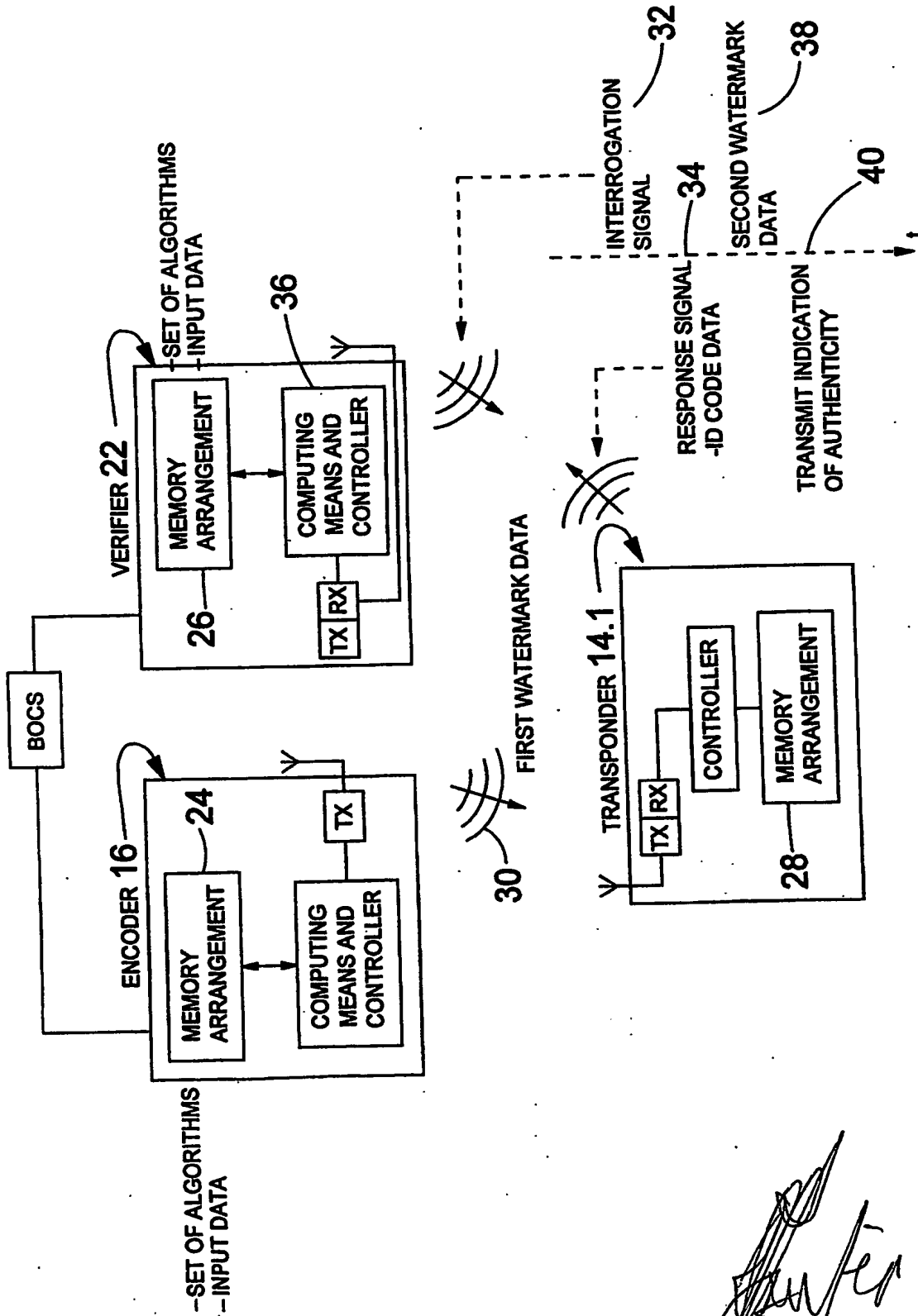


FIGURE 1

SUPERSENSOR (PTY) LTD



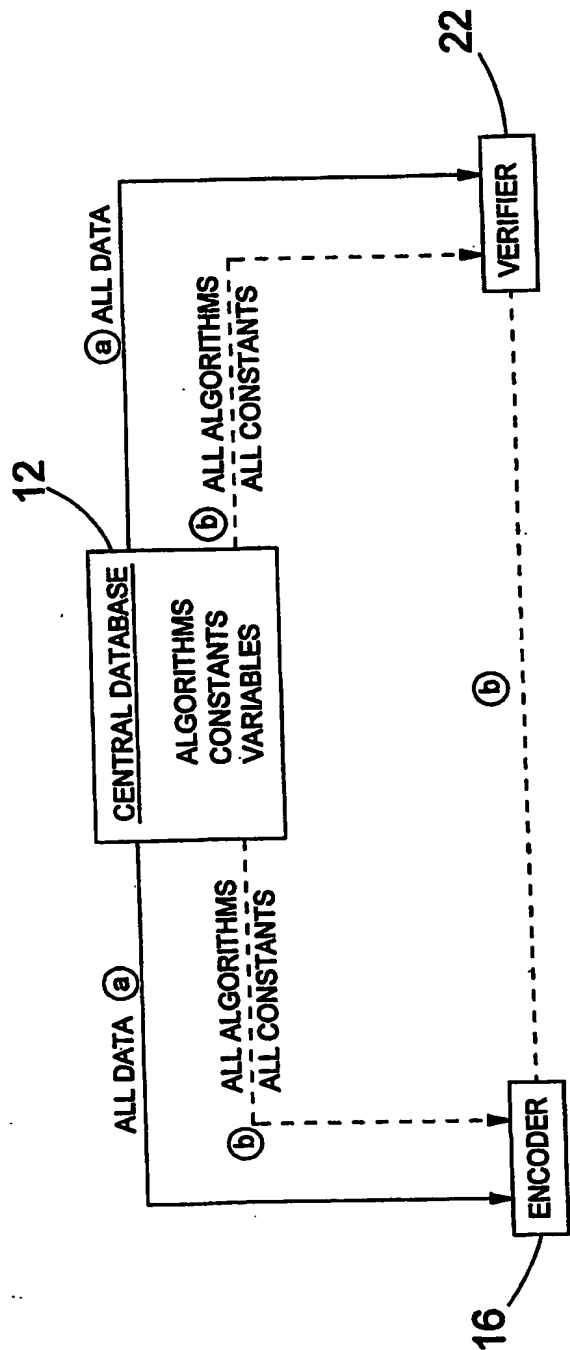


FIGURE 3



This Page is inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☒ BLACK BORDERS
- ☒ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☒ FADED TEXT OR DRAWING
- ☐ BLURED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☒ COLORED OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REPERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning documents *will not* correct images  
problems checked, please do not report the  
problems to the IFW Image Problem Mailbox**